IN THE SPECIFICATION:

Please amend Page ~~11~~ 14, the first paragraph, to read as follows:

Fig. 1 is a block diagram illustrating functions related to ~~claims 1 to 3 according to~~ the present invention;

Please amend Page ~~11~~ 15, the second paragraph, to read as follows:

Fig. 2 is a block diagram illustrating functions related to ~~claim 4 according to~~ another embodiment of the present invention;

Please amend Page ~~11~~ 15, the last paragraph, to read as follows:

Fig. 2 is a block diagram illustrating the system configuration of a cipher strength estimating device according to this embodiment. The cipher strength estimating device is, for example, a general-purpose computer as shown and includes a CPU 101, internal memory 102, an external storage unit 103 such as HDD, a communication interface 104, such as a modem, for providing connection to a communication network, a display 105, input means 106 such as a mouse or a keyboard, and the like, as shown in Fig. 3. In one embodiment, as shown in Figure 1, the control unit 1 interoperates with the putative untransformed text calculating unit 2. The putative untransformed calculating unit 2 comprises a putative untransformed text calculating unit body 2A and a session key prospect calculating section 2B. The putative untransformed calculating unit 2 can receive a putative transformed text and a plaintext and can output a putative untransformed text. The session key prospect calculating section 2B can receive the plaintext and the putative transformed text and can output a session key prospect to the putative untransformed text calculating unit body 2A. The session key prospect calculating section 2B can also receive recalculating request data from the control unit 1 and can also output

CH 1/14/08

uncalculability identifier data to the control unit 1. The putative untransformed text calculating text body can receive the putative transformed text and the session key prospect and can output the putative untransformed text.

Please amend Page ~~12~~ 16, first paragraph, to read as follows:

CH 1/14/08

In [[this]] another embodiment, by installing a predetermined program in the cipher strength estimating device and causing the CPU 101 and the peripheral devices to cooperate with each other, the cipher strength estimating device functions as a plaintext and ciphertext calculating unit 3, control unit 1, first putative untransformed text calculating unit 21, second putative untransformed text calculating unit 22, untransformed text calculating unit body 20A, first session key prospect calculating section 21K, and second session key prospect calculating section 22K, as shown in Fig. 4.